REMARKS

Claims 1, 14-20, 22-32, and 34 are pending in this application.

Applicants have amended claims 1, 14-20, 22-32, and 34, and have canceled claims 21 and 33. These changes do not introduce any new matter.

Objection to the Specification

In response to the objection to the specification based on inappropriate content in the Abstract, Applicants have provided a new Abstract of the Disclosure. Accordingly, Applicants request that the objection to the specification be withdrawn.

Claim Objections

In response to the objection to claims 14-26, 28, 29, 31, 33, and 34 (as noted above, claims 21 and 33 have been canceled), Applicants have amended claims 14-20, 22-26, 28, 29, 31, and 34 to correct the informalities noted by the Examiner. Accordingly, Applicants request that the objection to claims 14-20, 22-26, 28, 29, 31, and 34 be withdrawn.

Rejection Under 35 U.S.C. § 112

In response to the rejection of claims 17 and 25 under 35 U.S.C. § 112, second paragraph, as being indefinite, Applicants have amended claim 17 to recite "a safeguard value" and have amended claim 25 to recite "an error freedom." Applicants submit that claims 17 and 25 now satisfy the definiteness requirement of 35 U.S.C. § 112, second paragraph, and request that the rejection of these claims thereunder be withdrawn.

Rejection under 35 U.S.C. § 101

Applicants respectfully request reconsideration of the rejection of claims 1, 14-20, and 26-34 under 35 U.S.C. § 101 as being directed toward non-statutory subject matter (as noted above, claim 33 has been canceled). In response to the Examiner's concerns regarding non-statutory subject matter, Applicants have amended independent claims 1 and 27 to specify that the cryptographic calculation is one of a decryption in an RSA method and a signature

generation in an RSA method. This feature was specified in claim 21, which the Examiner did not include in the section 101 rejection (in light of the changes to claim 1, claim 21 has been canceled). Applicants have also amended independent claim 30, which now defines a computer program product including a computer-readable storage medium having a computer program stored thereon, to specify that the cryptographic calculation is one of a decryption in an RSA method and a signature generation in an RSA method. Applicants have amended independent claim 32 to specify that the data carrier is one of a smart card and a chip module, as well as to specify that the cryptographic calculation is one of a decryption in an RSA method and a signature generation in an RSA method. Accordingly, Applicants submit that claims 1, 14-20, 26-32, and 34 now define statutory subject matter under 35 U.S.C. § 101, and request that the rejection of these claims thereunder be withdrawn.

Rejection Under 35 U.S.C. § 102

Applicants respectfully request reconsideration of the rejection of claims 1, 14, 15, 19, 20, 27, 30, 32, and 33 under 35 U.S.C. § 102(b) as being anticipated by *Walmsley et al.* ("*Walmsley*") (US 2003/0159036 A1, which corresponds to WO 01/61918 A1) (as noted above, claim 33 has been canceled). As will be explained in more detail below, the *Walmsley* reference does not disclose each and every feature of independent claims 1, 27, 30, and 32, as amended herein.

Considering first independent claim 1, the *Walmsley* reference does not disclose each and every feature of the subject matter defined in present claim 1 for at least three reasons. First, the *Walmsley* reference does not disclose (or suggest) a key with at least two key parameters. The *Walmsley* reference discloses a validation protocol for determining whether an untrusted authentication chip is valid. *Walmsley* teaches two keys, which are named K_1 and K_2. The first key K_1 is a 160-bit secret key that is used to transform a value R during the authentication protocol (see Paragraph [0934]). The second key K_2 is a 160-bit secrecy key

that is used to transform a value M|R during the authentication protocol (see Paragraph [0939]).

The keys K_1 and K_2 are independent from each other and are used in different operations. *Walmsley* emphasizes that the security of the authentication chip depends on K_1 and K_2 being generated in a way that is non-deterministic (see Paragraphs [0936] and [0941]). *Walmsley* even considers a computer-run random number generator as too cryptographically weak for generating the keys K_1 and K_2. Instead, *Walmsley* recommends using physically generated random numbers (e.g., generated by a person tossing coins) for the keys K_1 and K_2 (see Paragraphs [0936] and [0941]).

In view of the foregoing, it cannot reasonably be said that keys K_1 and K_2 are two key parameters of a key, as specified in the claimed subject matter. The recitation of "a key with at least two key parameters" requires that the key parameters in some way form an overall key for the cryptographic calculation. This is not the case in the *Walmsley* reference, where the two keys K_1 and K_2 are entirely distinct and are used in two different cryptographic calculations. Moreover, *Walmsley* does not disclose that any one of the two keys K_1 and K_2 has at least two key parameters. Thus, the *Walmsley* reference does not disclose (or suggest) a key with at least two key parameters, as specified in the claimed subject matter.

Second, the *Walmsley* reference does not disclose (or suggest) preventing a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter. As discussed above, the *Walmsley* reference does not disclose a key with at least two key parameters. Thus, the *Walmsley* reference necessarily does not disclose preventing a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter. However, even if, for the sake of discussion, the keys K_1 and K_2 of *Walmsley* were considered to be the equivalent of the claimed key parameters, the *Walmsley* reference still would not

disclose this feature. As described above, the keys K_1 and K_2 are entirely separate. They are randomly generated independently from one another, and they are used in distinct operations. As such, any disturbance of one of the keys and the corresponding computation would not allow an attacker to draw any conclusion about the other key, and nothing in the *Walmsley* reference teaches or suggests such a possibility.

Moreover, the language of claim 1 refers to a corruption of one of the key parameters, and not to a mere observation of data or a corruption of any calculation steps. With regard to this feature, the Examiner relies on Paragraphs [0301]-[0303] and [0312] of *Walmsley*. The cited paragraphs of *Walmsley* describe several known attack methods as follows:

a) Paragraphs [0300] and [0301] describe that gate state changes may be spied out by observing infrared light bursts caused by such gate state changes. However, this is a mere *observation* of the *program execution*, and not any corruption of a key parameter.

b) Paragraphs [0302] and [0303] describe that AC signals (which may be part of a key) may be spied out using a non-invasive testing device, namely a Scanning Electric Potential Microscope (SEPM). However, this is a mere *observation* of the signals, and not any corruption of a key parameter.

c) Paragraph [0312] describes a possible attack in which a race condition is created at a certain moment in the algorithm execution. *Walmsley* concludes that this attack could lead to "revealing information about the key (or in the worst case, the key itself)." Again, this is a mere *spying out* of the key, and not any corruption of a key parameter.

Thus, in view of the foregoing, the *Walmsley* reference does not teach (or suggest) the preventing of a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter.

Third, the *Walmsley* reference does not disclose (or suggest) that the cryptographic calculation is one of a decryption in an RSA method and a signature generation in an RSA

method. On page 9 of the Office Action (in connection with the discussion of claim 21), the Examiner acknowledges that "Walmsley fails to teach wherein the cryptographic calculation is one of a decryption in an RSA method and a signature generation in an RSA method." Thus, the *Walmsley* reference does not disclose (or suggest) this feature of the presently claimed subject matter.

For at least the foregoing three reasons, the *Walmsley* reference does not disclose each and every feature of subject matter defined in present claim 1.

Applicants have amended each of independent claims 27, 30, and 32 along the same lines that claim 1 has been amended. As such, the arguments set forth above regarding present claim 1 also apply to present claims 27, 30, and 32.

Accordingly, independent claims 1, 27, 30, and 32, as amended herein, are patentable under 35 U.S.C. § 102(b) over *Walmsley*. Claims 14, 15, 19, and 20, each of which depends from claim 1, are likewise patentable under 35 U.S.C. § 102(b) over *Walmsley* for at least the same reasons set forth above regarding claim 1.

Rejection Under 35 U.S.C. § 103

Applicants respectfully request reconsideration of the rejection of claims 16-18, 21-26, 28, 29, 31, and 34 under 35 U.S.C. § 103(a) as being unpatentable over *Walmsley* in view of *Ngo et al.* ("*Ngo*") (US 2003/0097628 A1) and *Boneh et al.* ("*Boneh*") (US 6,965,673 B1) (as noted above, claim 21 has been canceled). Each of claims 16-18 and 22-26 ultimately depends from independent claim 1, each of claims 28 and 29 depends from independent claim 27, claim 31 depends from independent claim 30, and claim 34 depends from independent claim 32. The deficiencies of the *Walmsley* reference relative to the subject matter defined in present independent claims 1, 27, 30, and 32 are discussed above in connection with the anticipation rejection. Neither the *Ngo* reference nor the *Boneh* reference cures the above-discussed deficiencies of the *Walmsley* reference relative to the subject matter defined in

present claims 1, 27, 30, and 32. Accordingly, claims 16-18, 22-26, 28, 29, 31, and 34 are patentable under 35 U.S.C. § 103(a) over *Walmsley* in view of *Ngo* and *Boneh* for at least the reason that each of these claims ultimately depends from one of claims 1, 27, 30, and 32.

Further, with regard to the features of former claim 21 (which are now incorporated in the present independent claims), the Examiner alleges that these features are shown in the *Boneh* reference, and that it would have been obvious combine the *Walmsley* and *Boneh* references for the reasons set forth on page 9 of the Office Action. To the extent that this aspect of the obviousness rejection may be considered to be applicable to the present independent claims, Applicants respond as follows.

The *Walmsley* reference is concerned with a validation protocol that uses *symmetric* cryptographic functions (see Paragraphs [0335]-[0346]). On the other hand, the *Boneh* reference is concerned with *asymmetric* cryptographic functions according to the RSA method. It is well known to those skilled in the cryptographic arts that symmetric and asymmetric cryptographic functions constitute vastly different fields and that concepts used in one of these fields cannot be interchangeably used in the other field. As such, one having ordinary skill in the art would not have had a reasonable expectation that any meaningful result could be obtained by combining the *Walmsley* and *Boneh* references in the manner proposed by the Examiner.

Moreover, the *Boneh* reference, like the *Walmsley* reference, does not teach or suggest the preventing of a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter. At column 8, lines 41-45, the attack that is addressed in the *Boneh* reference is described as follows:

> This erroneous signature may be generated, for example, while a tamper proof device 200 is placed under physical stress, such as being placed in an extreme environment, which is likely to cause hardware faults.

The attack contemplated by *Boneh* is a so-called fault attack in which the *calculation steps* of exactly one branch of the RSA calculation are disturbed by an external influence such as, for example, heat or radiation or electrical pulses. This kind of attack, which is also known by the name "Bellcore attack," is acknowledged and discussed in detail in Paragraphs [0005] and [0006] of the subject application. However, as set forth in Paragraph [0010] of the subject application, the claimed subject matter is based on the insight that an attack similar to the Bellcore attack is possible not only by interfering with the calculation process during the cryptographic calculation, but *also by supplying the cryptographic calculation with incorrect key parameters*. The claimed subject matter strives to provide protection against these kind of attacks, i.e., protection against attacks "in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter," as specified in the present claims. The *Boneh* reference does not disclose or fairly suggest this claimed feature.

The *Boneh* reference also does not disclose or suggest the performing of an integrity check of the key. The primary teaching of Boneh is a description of various attack schemes. The *Boneh* reference discusses possible countermeasures to such attacks only in passing in column 17 of the reference. The proposed countermeasures include checking the *output* of a computation before releasing it, checking intermediate results held in internal *registers* of the cryptography device, and using blinding operations. As such, *Boneh* does not teach or fairly suggest the performing of an integrity check of the key, as specified in the presently claimed subject matter.

In summary, one having ordinary skill in the art would not have been motivated to combine the *Walmsley* and *Boneh* references in the manner proposed by the Examiner. However, even if these references were to be combined in the proposed manner, this combination would not have resulted in a method, computer program product, or portable data carrier having each and every feature of the presently claimed subject matter. As such,

the combination of *Walmsley* in view of *Boneh* would not have rendered the subject matter defined in present claims 1, 27, 30, and 32 obvious to one having ordinary skill in the art.

Conclusion

In view of the foregoing, Applicants respectfully request reconsideration and reexamination of claims 1, 14-20, 22-32, and 34, as amended herein, and submit that these claims are in condition for allowance. Accordingly, a notice of allowance is respectfully requested. In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at **(408) 749-6902**. If any additional fees are due in connection with the filing of this paper, then the Commissioner is authorized to charge such fees to Deposit Account No. 50-0805 (Order No. WACHP006).

Respectfully submitted,
MARTINE PENILLA & GENCARELLA, L.L.P.

/Peter B. Martine/

Peter B. Martine
Reg. No. 32,043

710 Lakeway Drive, Suite 200
Sunnyvale, California 94085
Customer Number 25920